IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Fabio R. Maino, et al.	Attorney Docket No.: ANDIP004/425452
Application No.: 10/034,367	Examiner: TESLOVICH, TAMARA
Filed: December 27, 2001	Group: 2437
Title: METHODS AND APPARATUS FOR SECURITY OVER FIBRE CHANNEL	Confirmation No: 8712

CERTIFICATE OF EFS-WEB TRANSMISSION
I hereby certify that this correspondence is being transmitted electronically through EFS-WEB to Mail Stop AF, Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on October 8, 2009.

Signed: /Latonia Ervin/
Latonia Ervin

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Please consider the following remarks and arguments:

Claims 1-48 are pending. Claims 1-25 have been withdrawn from consideration. Claims 26-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hawe (USPN 5,070,528) in view of Hagerman (USPN 6,973,568).

All independent claims 26, 36, and 48 include recitations not taught or suggested by the references cited by the Examiner either alone or in combination. For example, the independent claims all variably recite a first fibre channel frame including a security enable indicator wherein the first fibre channel frame is associated with a fabric login or a port login message. The independent claims also all variably recite a security control indicator in a second fibre channel frame, wherein the security control indicator is used to determine if the frame is encrypted and authenticated. In some instances, the frames are transmitted. In other instances, the frames are

received. The materials cited by the Examiner either alone or in combination do not teach or suggest these recitations.

The Examiner argues that Hawes describes a cryptographic preamble "that includes an offset field to indicate the location of data to be cryptoraphically processed as well as a mode field indicating the type of cryptographic processing to be performed." It is acknowledged that Hawes describes a cryptographic preamble. The Examiner appears to argue that the cryptographic preamble can be both the security enable indicator in a first frame and the security control indicator in a second frame. It is respectfully submitted that although the cryptographic preamble may teach or suggest a security control indicator, it is not a security enable indicator.

The Specification explicitly describes a security enable indicator as being a separate and distinct entity from a security control indicator. The security enable indicator is used during an initialization sequence to show whether a newly introduced node supports security. "Any indicator showing that the frame is secure is referred to herein as a security control indicator. It should also be noted that this is distinct from the above mentioned security enable indicator, which is used during an initialization sequence to show whether a newly introduced node supports security." (page 20, lines 3-6) The cryptographic preamble in Hawes may indicate that a particular frame is secure, but does not in any way indicate that a newly introduced node supports security.

Hawes appears to assume that all network nodes support security and consequently, no security enable indicator is needed in the Hawes system.

The independent claims variably recite "identifying a security enable parameter in the first frame; transmitting an acknowledgment to the second network entity that the first network entity supports security, the acknowledgment including algorithm information." After it is recognized that the first network entity supports security is there identification of "a security control indicator in the second frame from the second network entity, wherein the security control indicator is used to determine if the second frame is encrypted and authenticated."

Furthermore, it is respectfully submitted that none of the materials teach or suggest including any security enable indicator in the first frame where the first frame is associated with "a fabric login or port login message" as recited in the independent claims. Transmitting a

cryptographic preamble in a fabric login or port login message to a node that does not support security may cause deleterious effects. Hagerman is not believed to teach or suggest using any login, fabric login, port login, flogi, or plogi messages to include a security enable indicator. Hawes does not use any fabric login or port login messages because Hawes describes a packet network system that does not have any fabric login or port login mechanisms.

According to various embodiments, "The techniques of the present invention include security in initialization messages such as PLOGI, FLOGI, and other classes of messages such as SW_ILS, FC-CT, ELS and ELP. According to various embodiments, the techniques of the present invention embed a security enable parameter in an authentication message. When a new network entity is introduced into a fibre channel fabric, the new network entity transmits an initialization message with the security enable parameter. The receiving network entity may or may not support security. If the receiving network entity supports authentication, the receiving network entity can extract the security enable parameter and transmit a response acknowledging authentication capabilities. Other information can be exchanged during an authentication sequence to provide for future security in transmissions between the two network entities. In one example, the two entities can exchange cryptographic material in the authentication sequence to allow common key generation." (page 11, lines 19-31)

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/Audrey Kwan/

G. Audrey Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100

APPENDIX: IN THE CLAIMS

1. (Withdrawn) A method for authenticating network entities in a fibre channel network, the method comprising:

receiving a fibre channel authentication message from a first network entity at a second network entity in a fibre channel network, wherein the authentication message provides information for authenticating or reauthenticating the first network entity in the fibre channel network;

determining that both the first network entity and the second network entity support security;

verifying that the first network entity corresponds to an entry in an authentication table associated with the second network entity;

receiving first network entity verification information that confirms the identify of the first network entity.

2. (Withdrawn) The method of claim 1, further comprising generating a session key at the second network entity, wherein the session key is generated using public information associated with the first network entity and a random parameter.

3. (Withdrawn) The method of claim 1, further comprising:
exchanging security association parameters such as the SPI and the algorithm identifier.

4. (Withdrawn) The method of claim 1, wherein the authentication message is associated with a request for a fabric login.

5. (Withdrawn) The method of claim 1, wherein determining that both the first and second network entities support security comprises identifying a security enable parameter in the initialization message.

6. (Withdrawn) The method of claim 1 further comprising determining which authentication and key exchange protocol are supported by the two entities.

7. (Withdrawn) The method of claim 2, wherein the public information associated with the first network entity is provided to the second network entity by the first network entity.

8. (Withdrawn) The method of claim 2, wherein the session key generated at the second network entity is also generated at the first network entity using public information associated with the second network entity and a random parameter provided by the second network entity.

9. (Withdrawn) The method of claim 8, wherein the public information associated with the second network entity is provided to the first network entity by the second network entity.

10. (Withdrawn) The method of claim 8, wherein first network entity verification information is generated at the first network entity using public information associated with the first and second network entities and the session key.

11. (Withdrawn) The method of claim 10, further comprising verifying that the first network entity verification information received corresponds to verification information generated at the second network entity using public information associated with the first and second network entities and the session key.

12. (Withdrawn) The method of claim 11, further comprising transmitting second network entity verification information to the first network entity, wherein the second network entity verification information is generated at the second network entity using public information associated with the first network entity, the first network entity verification information, and the session key.

13. (Withdrawn) The method of claim 12, wherein the second network entity verification information transmitted corresponds to second network entity verification information generated at the first network entity using public information associated with the first network entity, the first network entity verification information, and the session key.

14. (Withdrawn) The method of claim 8, wherein the second network entity is a storage device in a storage area network.

15. (Withdrawn) The method of claim 8, wherein the first and second network entities are domain controllers in a storage area network.

16. (Withdrawn) The method of claim 8, wherein the first and second network entities are switches.

17. (Withdrawn) The method of claim 8, wherein the first network entity is a host.

18. (Withdrawn) The method of claim 17, wherein the second network entity is a storage device.

19. (Withdrawn) The method of claim 8, wherein the authentication message is a fibre channel authentication message.

20. (Withdrawn) The method of claim 19, wherein the authentication message is a login message.

21. (Withdrawn) The method of claim 20, wherein the authentication message is a PLOGI or FLOGI message.

22. (Withdrawn) The method of claim 8, further comprising:

storing security association information associated with the first network entity.

23. (Withdrawn) The method of claim 8, further comprising:

transporting security association information in the messages exchanged between the two network entities

24. (Withdrawn) The method of claim 22, wherein security association information comprises an identifier associated with the first network entity and the session key.

25. (Withdrawn) The method of claim 24, wherein security association information further comprises an encryption algorithm identifier and an authentication algorithm identifier.

26. (Previously Presented) A method for processing frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

receiving a first frame at the first network entity from the second network entity in the fibre channel network, wherein the first frame is associated with a fabric login or port login message;

identifying a security enable parameter in the first frame;

transmitting an acknowledgment to the second network entity that the first network entity supports security, the acknowledgment including algorithm information;

receiving a second frame at the first network entity from the second network entity;

identifying a security control indicator in the second frame from the second network entity, wherein the security control indicator is used to determine if the second frame is encrypted and authenticated;

determining that a security association identifier associated with the second frame corresponds to an entry in a security database;

decrypting a first portion of the second frame by using algorithm information contained in the entry in the security database.

27. (Original) The method of claim 26, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

28. (Original) The method of claim 27, wherein the first portion is decrypted using a key contained in the entry in the security database.

29. (Original) The method of claim 27, wherein the first portion is encrypted using DES, 3DES or AES.

30. (Previously Presented) The method of claim 27, further comprising:

recognizing that a second portion of the second frame supports authentication;

using algorithm information contained in the entry in the security database to authenticate the second portion of the second frame.

31. (Original) The method of claim 30, wherein the second portion is authenticated using MD5 or SHA1.

32. (Original) The method of claim 30, wherein the authentication sequence is a fibre channel login sequence between the first and second network entities.

33. (Original) The method of claim 32, wherein the login sequence is a PLOGI or FLOGI sequence.

34. (Original) The method of claim 32, wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence.

35. (Original) The method of claim 32, wherein the first and second network entities are domain controllers and the authentication sequence is a SW_ILS sequence.

36. (Previously Presented) A method for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

transmitting a first fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity, the first fibre channel frame including a security enable indicator, wherein the first fibre channel frame is associated with a fabric login or a port login message;

receiving an acknowledgment from the second network entity indicating that the second network entity supports security;

inserting key and algorithm information from the second network entity into a security database;

identifying a second fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

determining if the second fibre channel frame corresponds to the selectors of an entry in a security database;

encrypting a first portion of the second fibre channel frame using key and algorithm information associated with the entry in the security database;

providing a security control indicator in the second fibre channel frame, wherein the security control indicator is used to determine if the frame is encrypted and authenticated;

transmitting the second fibre channel frame to the second network entity.

37. (Original) The method of claim 36, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

38. (Original) The method of claim 36, wherein the payload is encapsulated using the Authentication Header protocol or the Encapsulating Security Payload protocol.

39. (Previously Presented) The method of claim 38, further comprising adding security information to the header of the second fibre channel frame.

40. (Previously Presented) The method of claim 37, wherein a first portion of the second fibre channel frame is encrypted using DES, 3DES, or AES.

41. (Previously Presented) The method of claim 37, wherein parameters in the header are normalized prior to encrypting the first portion of the second fibre channel frame.

42. (Previously Presented) The method of claim 41, wherein the payload is padded prior to encrypting the first portion of the second fibre channel frame.

43. (Previously Presented) The method of claim 37, further comprising:

computing authentication data using key and algorithm information as well as a second portion of the second fibre channel frame.

44. (Original) The method of claim 43, wherein authentication data is computed using MD5 or SHA1.

45. (Original) The method of claim 43, wherein the authentication sequence is a fibre channel login sequence between the first and second network entities.

46. (Original) The method of claim 45, wherein the login sequence is a PLOGI or FLOGI sequence.

47. (Original) The method of claim 45, wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence or an SW_ILS message.

48. (Previously Presented) An apparatus for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the apparatus comprising:

means for transmitting a first fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity, the first fibre channel frame including a security enable indicator, wherein the first fibre channel frame is associated with a fabric login or a port login message;

means for receiving an acknowledgment from the second network entity indicating that the second network entity supports security;

means for inserting key and algorithm information from the second network entity into a security database;

means for identifying a second fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

means for determining if the second fibre channel frame corresponds to the selectors of an entry in a security database;

means for encrypting a first portion of the second fibre channel frame using key and algorithm information associated with the entry in the security database;

means for providing a security control indicator in the second fibre channel frame, wherein the security control indicator is used to determine if the frame is encrypted and authenticated;

means for transmitting the second fibre channel frame to the second network entity.

49. (Canceled)

50. (Canceled)